PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 17/60

A1

(11) International Publication Number: WO 99/05628

(43) International Publication Date: 4 February 1999 (04.02.99)

(21) International Application Number: PCT/US98/15190

(22) International Filing Date: 22 July 1998 (22.07.98)

(30) Priority Data:
08/898,563 22 July 1997 (22.07.97) US

(71) Applicant: UNISYS CORPORATION [US/US]; Township Line and Union Meeting Roads, P.O. Box 500, Blue Bell, PA 19424-0001 (US).

(72) Inventor: SMORODINSKY, Lev; 25121 Grissom Road, Laguna Hills, CA 92653 (US).

(74) Agent: STARR, Mark; Unisys Corporation, Township Line and Union Meeting Roads, P.O. Box 500, Blue Bell, PA 19424-0001 (US).

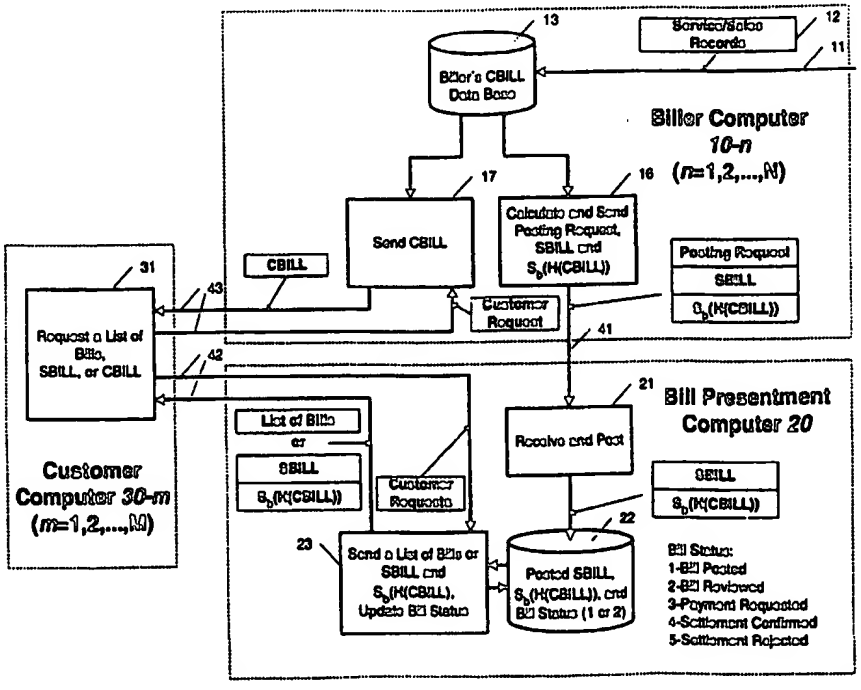
(81) Designated States: CA, JP, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: ELECTRONIC BILL PRESENTMENT AND PAYMENT SYSTEM WHICH DETERS CHEATING BY EMPLOYING HASHES AND DIGITAL SIGNATURES

(57) Abstract

An electronic bill presentment and payment system (Fig. 1) includes multiple biller computers (10–n), a bill presentment computer (20), and multiple customer computers (30–m). Each biller computer stores complete bills (CBILL) for the customer of a corresponding biller, and the bill presentment computer stores a respective summary (SBILL) of each complete bill along with a hash of that complete bill which is digitally signed by the biller computer $S_b(H(CBILL))$. Each particular customer computer makes a payment on a selected complete bill by generating a payment message (step S24 of Fig. 4) which includes: a) the hash of the selected complete bill digitally signed by the biller computer; and b) an authorization to pay a specified amount of funds on the selected complete bill, both of which are digitally signed by that particular customer computer $S_c[\$X,S_b(H(CBILL))]$. This payment message is stored in a closing record for use in resolving issues regarding whether or not the bill was changed after payment was authorized, and whether or not an alleged payment on the selected bill was authorized.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

TITLE: ELECTRONIC BILL PRESENTMENT AND PAYMENT SYSTEM WHICH DETERS CHEATING BY EMPLOYING HASHES AND DIGITAL SIGNATURES

BACKGROUND OF THE INVENTION:

This invention relates to electronic systems by which bills are presented and paid.

One prior art bill presentment and payment system is disclosed in Fig. 1 of U.S. Patent 5,465,206 (hereinafter the Visa patent). In this system, a customer receives a bill from a biller; and in response, the customer mails a check back to the biller. This check is then presented by the biller to the biller's bank for payment. Then the biller's bank sends the check to a settlement bank which clears and settles the transfer of funds between the biller's bank and the customer's bank. Following this settlement step, funds are transferred by the biller's bank to the biller's account where it is available for withdrawal.

In a second prior art bill presentment and payment system (which is disclosed in Figs. 2A & 2B of the Visa patent), a customer responds to a bill from a biller by electronically sending a message to a service bureau, and this electronic message authorizes the service bureau to pay the bill. Upon receipt of the

message, the service bureau writes a check on the customer's account in the customer's bank and presents that check to the service bureau's bank for payment. Then, the service bureau's bank sends the check to a settlement bank which clears and settles the transfer of funds between the service bureau's bank and the customer's bank. This sequence of steps is repeated many times for many customers of the biller. Thereafter, the service bureau sends the biller a list of all of the bills that were paid along with a single check for the total amount paid.

In a third prior art bill presentment and payment system (which is disclosed in Fig. 3 of the Visa patent), a biller obtains regular periodic payments from a customer's account in a customer's bank with those payments being initiated by the biller, rather than the customer. With this method, the biller maintains a file which identifies the customer, the amount of the periodic payment, and the date on which each payment is due. To initiate each payment, the biller electronically sends a request for payment to the biller's bank; and in response, the biller's bank generates a debit request in a certain standard format, which is required by an automated clearing house (ACH). This debit request is then stored in the biller's bank, along with all other ACH debit and credit requests which the biller's bank generates for other customers. Thereafter, a batch of ACH debit and credit requests are electronically transmitted to the Federal Reserve or other ACH clearing

institution; and by this transmission, net accounts between the biller's bank and the customer's bank are settled.

In a fourth prior art bill presentment and payment system (which is disclosed in Figs. 4-12 of the Visa patent), the biller's bank, the customer's bank, and a settlement bank are all intercoupled by an electronic payment network. With this method, a customer responds to a bill from a biller by ordering the customer's bank to pay the bill. In response, the customer's bank examines the customer's account to determine if sufficient funds are available to pay the bill or determine that the customer's bank is willing to take the risk of loss if funds are not available. If either determination is made, the customer's bank electronically sends a payment message through the payment network to the biller's bank. Each such payment message is also stored in the payment network where it is acted upon by a settlement subsystem which nets the funds that are being transferred by all payment messages between the customer's bank and the biller's bank. Thereafter, the settlement subsystem electronically sends a transfer order to the settlement bank which settles the net accounts between the customer's bank and the biller's bank. By this settlement step, funds are transferred by the biller's bank to the biller's account.

However, a major drawback in all of these prior art systems is that no means is provided for electronically presenting the bill to the customer before

it is paid. In the systems of Figs. 1, 2, and 4, the bill is physically sent to the customer by conventional post office mail; and in the system of Fig. 3, the bill is paid without ever being sent to the customer.

Further, if the above prior art systems were somehow modified such that the bill was sent electronically rather than by mail, then a new problem would arise because the customer would not have any documentation from the biller to establish the amount of the bill. Consequently, after a payment is made by the customer, a biller could increase the amount due in the bill and claim that the increased amount was in the original bill.

Also, if the above prior art systems were somehow modified such that checks are eliminated and all payments occur electronically, then another new problem arises in that no canceled checks are generated to establish the amount of payment which was authorized. Consequently, after payment of a certain amount of funds is made electronically, a customer can subsequently claim that only a smaller payment was authorized and/or a biller can subsequently claim that a larger payment was authorized.

Accordingly, a primary object of the present invention is to provide an all electronic bill presentment and payment system which employs hashes and digital signatures to avoid cheating by a biller and/or customer.

BRIEF SUMMARY OF THE INVENTION:

An all electronic bill presentment and payment system, which constitutes one preferred embodiment of the present invention, includes a biller computer having a data base which stores a plurality of complete bills for a plurality of customers, and a bill presentment computer, coupled to the biller computer, having a data base which stores a summary of each complete bill and a respective hash of each complete bill which is digitally signed by the biller computer. Also, this embodiment includes multiple customer computers, coupled to the biller computer and the bill presentment computer; and each particular customer computer – a) can request and receive from the bill presentment computer, a summary of a selected complete bill plus its respective digitally signed hash, and b) can request and receive from the biller computer, the selected complete bill.

To ensure that the selected complete bill in the biller computer was not changed after the summary of that complete bill was stored in the bill presentment computer, the particular customer computer generates a new hash of the selected complete bill as received from the biller computer, and decrypts the digitally signed hash of the selected complete bill as received from the bill presentment computer. If the new hash does not equal the decrypted hash, the customer computer displays a message indicating that the bill should not be paid because the discrepancy exists.

If the new hash and the decrypted hash are equal, then a payment message can be sent from the particular customer computer to the bill presentment computer; and this payment message includes -a) the digitally signed hash of the selected complete bill, and b) an authorization to pay a specified amount of funds on the selected complete bill, both of which are digitally signed by the particular customer computer. Preferably this payment message is stored in the database of the bill presentment computer and in a closing record of an electronic payment subsystem which couples to the bill present computer.

Thereafter, the stored payment message can be used to resolve certain disputes which may arise between the biller and the customer. If the issue in the dispute is whether or not the bill was changed after payment was authorized, then this is resolved by a dispute resolving means which: reads from the closing record, the hash of the selected complete bill which is digitally signed by the biller computer and the particular customer computer; decrypts the digitally signed hash to thereby obtain the hash in an unsigned form; generates a new hash of the complete bill as currently stored in the biller computer; and, compares the new hash to the decrypted hash in unsigned form. A miscompare indicates that the complete bill was changed after payment was authorized.

If the issue in the dispute is whether or not an alleged payment was made on the selected bill, then this is resolved by the dispute resolving means which:

reads from the closing record, the authorization to pay the specified amount of funds which is digitally signed by the particular customer computer; decrypts the digitally signed authorization to thereby obtain the specified amount of funds in an unsigned form; and, compares the unsigned specified amount of funds to the alleged payment. If a miscompare occurs, the alleged payment was not authorized and thus did not occur.

Preferably, each digitally signed hash consists of sixteen to thirty-two bytes; whereas each complete bill typically consists of thousands of bytes. Consequently, by storing the hash of the complete bill rather than the entire complete bill, the total amount of storage is greatly reduced in the data base of the bill presentment computer and in the closing records of the payment subsystem.

BRIEF DESCRIPTION OF THE DRAWINGS:

Fig. 1 shows an electronic bill presentment and payment system which constitutes one preferred embodiment of the present invention.

Figs. 2A & 2B together show an example of a complete bill, and such a complete bill is indicated in Fig. 1 as CBILL.

Fig. 3 shows an example of a summary of the complete bill of Figs. 2A & 2B, and such a summary is indicated in Fig. 1 as SBILL.

Fig. 4 shows various steps which are performed by a program 31 in the customer computer 30-m of Fig. 1.

Fig. 5 shows how the bill presentment and payment system of Fig. 1 interacts with a payment subsystem 50.

Fig. 6 shows how a payment closing record in the payment subsystem 50 of Fig. 5 is used by a computer Z, to help resolve disputes regarding the payment of a bill.

Fig. 7 shows two modifications to the bill presentment and payment system of Figs. 1-6.

Fig. 8 shows two additional modifications to the bill presentment and payment system of Figs. 1-6.

DETAILED DESCRIPTION:

In Fig. 1, an electronic bill processing system is shown which constitutes one preferred embodiment of the present invention. This Fig. 1 embodiment includes multiple biller computers 10-n (where n equals 1,2, . . . N), a single bill presentment computer 20, and multiple customer computers 30-m (where m equals 1,2, . . . M). All of these computers 10-n, 20, and 30-m are intercoupled by communication channels 41, 42 and 43 as shown.

Each biller computer 10-n has an input 11 on which it receives detailed sales and service data 12 for various customers; and this data 12 is stored in a database 13 within the biller computer 10-n. There, the data 12 is arranged as one or more complete bills for each customer. A particular complete bill is indicated in

Fig. 1 as CBILL, and an example of one typical CBILL is shown in Figs. 2A & 2B.

Inspection of the CBILL in Figs. 2A & 2B shows that it includes several lists 14a-14e of the individual items for which there is a charge. To save space in Figs. 2A & 2B, many of the individually billed items are replaced with a series of three dots; but in an actual CBILL, all of the individually billed items are shown. Also, the CBILL in Figs. 2A & 2B contains superfluous information such as an advertisement 15a, company logos 15b and 15c, a reminder 15d of a penalty which is incurred if the total amount due is not paid by a certain date, etc.

Each biller computer 10-n also includes a program 16 which operates on each CBILL in its database 13, as follows. First, the program 16 generates a summary of the complete bill, and this summary is indicated in Fig. 1 as SBILL. Fig. 3 shows an example of an SBILL for the CBILL in Figs. 2A & 2B. By extracting the superfluous information 15a-15d and replacing the lists 14a-14e with one total amount due, the SBILL of Fig. 3 is made at least twenty times shorter than the CBILL of Figs. 2A & 2B.

After the bill summary is generated, the program 16 generates a hash of the complete bill; and then the program 16 uses a biller computer private key to digitally sign the hash. This hash prior to signing is indicated in Fig. 1 as H(CBILL); the digitally signed hash is indicated in Fig. 1 as $S_b(H(CBILL))$; and S_b indicates the signing occurred with the private key " b" in the biller computer. Then, the program 16 sends a posting request to the bill presentment computer 20 which

contains the bill summary SBILL and the digitally signed hash $S_b(H(CBILL)$.

In the bill presentment computer 20, a program 21 is included which receives the bill summary SBILL and the digitally signed hash $S_b(H(CBILL))$. This program 21 then posts the bill summary SBILL and the digitally signed hash $S_b(H(CBILL))$ by storing them in a database 22 within the bill presentment computer. Also, the program 21 stores a bill status code of " 1" in the database 22 which indicates that the bill summary SBILL and the digitally signed hash $S_b(H(CBILL))$ are now posted.

Each customer computer 30-m includes a program 31, the details of which are shown in Fig. 4, that interacts with the bill presentment computer 20 and the biller computers 10-n. To begin, the program 31 receives a request from an operator of the customer computer 30-m to display a list of current unpaid bills (LCUB). In response, the customer computer performs step S1 of Fig. 4 in which the request is sent to the bill presentment computer 20. This request is received in the bill presentment computer by a program 23 which examines the database 22 and generates the requested list. Then, the requested list of current unpaid bills is sent to the customer computer 30-m where it is received and displayed by program 31, as indicated by step S2 in Fig. 4.

Thereafter, the operator of the customer computer 30-m can make a request to see a particular bill summary SBILL which is on the list. In response, the program 31 sends a request to the bill presentment computer for that particular bill summary as indicated by step S3 in Fig. 4. Then, program 23 in the bill presentment computer 20 obtains the requested bill summary, from the database 22, as well as the digitally

signed hash of the corresponding complete bill. That summary and signed hash are then sent to the customer computer, where they are received as step S4 in Fig. 4. Also, the bill presentment computer changes the status code of the bill summary which it sent to "2", to thereby indicate that the bill has been reviewed by the customer computer.

Next, in step S5 of Fig. 4, program 31 in the customer computer 30-m displays the bill summary which it receives. Then, based on what that bill summary shows, the operator of the customer computer 30-m has several options S6a-S6d on how to proceed. With option S6a, a request is made to display the complete bill which corresponds to the bill summary that is being displayed. With option S6b, a request is made for a payment subscreen whereby a selectable amount of funds can be paid on the bill whose summary is being displayed. With option S6c, step S1 can be returned to, whereupon the list of current unpaid bills will again be displayed. With option S6d, the interaction with the bill presentment computer 20 and biller computers 10-m can be terminated. These options are shown under the bill summary of Fig. 3; and a particular option is selected by moving a cursor via a mouse on the desired option and "clicking".

If option S6a is selected, the customer computer 30-m performs a subroutine 31a within the program 31 which includes steps S11-S15. In step S11, the customer computer 30-m sends a request to the biller computer 10-n for the particular complete bill which corresponds to the bill summary that is being displayed. Each biller computer includes a program 17, which responds to such the request by retrieving a complete

bill from its database 13 which should be the requested complete bill, and by sending the complete bill which was retrieved to the customer computer 30-m. This complete bill is received by subroutine 31a in the customer computer as step S12 in Figs. 2A & 2B.

Next, in step S13, the subroutine 31a uses a public key for the biller's computer to decrypt the digitally signed hash $S_b(H(CBILL))$. By this step, the hash of the complete bill is obtained in unencrypted form as H(CBILL). Then in step S14, the subroutine 31a recomputes a new hash on the complete bill which it obtained in step S12 from the biller's computer 10-n. Then in step S15, the subroutine 31a compares the decrypted hash of step S13 with the new recomputed hash of step S14.

If the two compared hashes are not equal, then a message is displayed which alerts the operator to the discrepancy. One potential cause for this discrepancy is that the complete bill in the biller's computer 10-n was changed after the summary of the complete bill CBILL and its digitally signed hash were posted in the bill presentment computer 20. Thus, by displaying the discrepancy message, the customer is protected against making a payment on a bill where the current complete bill as retrieved from the biller computer and its summary as posted in the bill presentment computer, do not agree.

Conversely, if the two compared hashes in step S15 are equal, then the requested complete bill is displayed on the customer computer 30-m. This occurs as step S20 in Fig. 4. Then, based on what the displayed complete bill shows, the operator of the customer

computer 30-m has several options S21a - S21c on how to proceed.

With option S21a, a request is made for a payment subscreen whereby a selectable amount of funds can be paid on the complete bill which is being displayed. With option S21b, the initial step S1 can be returned to whereupon the list of current unpaid bills will again be displayed. With option S21c, the interaction with the bill presentment computer 20 and biller computers 10-m can be terminated.

If option S21a is selected, then the customer computer 30-m performs step S22 wherein the operator of the customer computer 30-m enters an amount $X which is to be paid on the bill. Then by option S23, the operator can authorize such payment to be made. In reponse to that authorization, the customer computer performs step S24 wherein a payment request message (PRM) is sent to the bill presentment computer 20. This payment request message contains -a) the hash of the selected complete bill which was digitally signed by the biller computer, and b) an authorization to pay the specified amount of funds $X on the selected complete bill. Also, the program 31 uses a customer computer private key to digitally sign both of these items a) and b) and this is indicated in step S22 of Fig. 4 as $S_c[\$X, S_b(H(CBILL))]$. Here, S_c indicates the signing occurred with the private key " C" in the customer computer.

Due to the fact that the payment amount $X is signed by the customer computer as S_c in step S24, the biller is protected from a subsequent allegation by the customer that he paid a larger amount. Also, due to the fact that the hash of the complete bill is signed by the customer computer in step S24, the biller is protected

from a subsequent allegation by the customer that the amount of his bill has been changed.

Suppose now that in Fig. 4, the operator of the customer computer selects option S6b whereby a request is made for a payment subscreen on the bill summary, without seeing the complete bill. When option S6b is selected, the Fig. 4 program automatically performs the above described subroutine 31a. Then if a payment is authorized, the Fig. 4 program performs step S24. By performing subroutine 31a, the customer is again protected against making a payment on a bill where the complete bill and its summary do not agree. By performing step S24, the biller is again protected against the customer disputing the amount which he authorized to be paid and/or disputing the amount due in the bill which he received.

Referring next to Fig. 5, it shows how the payment request message PRM is processed by the bill presentment computer 20 in conjunction with an electronic payment subsystem 50. In this payment subsystem 50, each customer has an account which is maintained by a computer X(i) in the customer's bank, and each biller has an account which is maintained by a computer X(j) in the biller's bank. All of computers X(i) and X(j) are coupled to each other and to another computer Y which resides in a clearing and settlement bank.

When the payment request message PRM is sent from the customer computer 30-m, that message is received by a program 24 in the bill presentment computer 20. This occurs in Fig. 5 at time t1. Then, in response to the received payment request message, the program 24 accesses the data base 22 and changes the status of the bill that is to be paid to a code of " 3" , which

indicates that payment has been requested. This occurs at time t2 in Fig. 5.

Next, the program 24 in the bill presentment computer 20 sends the payment request message to the bank computer X(i) which maintains the account of the customer who authorized payment. There, the payment request message is received by a program 51a. This occurs at time t3 in Fig. 5. In response, the program 51a accesses a data base 51b in the customer computer X(i) which contains the account of the customer who authorized payment. By this step, the program 51a verifies that a sufficient amount of funds are in the customer's account to cover the authorized payment. This step occurs at time t4 in Fig. 5.

If sufficient funds are found, the computer X(i) sends a message to the computer X(j) in the bank for the biller who is to be paid. This message, which occurs at time t5 in Fig. 5, requests a verification of the account for the biller. In response, a program 52a in the computer X(j) accesses a data base 52b which contains the account of the particular biller who is to be paid. This occurs at time t6 in Fig. 5. Then the program 52a in the computer X(j) sends a return message back to the program 51a in computer X(i) which indicates whether or not the biller's account was found and is in order.

If the biller's account is in order, the computer X(i) sends a message to the clearing and settlement computer Y which requests that the transfer of funds which is authorized in the payment request message actually occur. This request, which is sent at time t7 in Fig. 5, is received by a program 53a in the computer Y. In response, the program 53a accesses a data base 53b which holds net accounts for the banks with computers

X(i) and X(j). If those accounts are in order, then program 53a subtracts the amount which is to be paid from the net account for the bank with computer X(i), and adds the amount to be paid to the net account for the bank with computer X(j). This occurs at time t8 in Fig. 5.

After the net accounts are changed as described above, then at time t9, program 53a accesses a data base 53c in which a closing record for the payment request messages is stored. This closing record includes a) the hash of the selected complete bill which was digitally signed by the biller computer 10-n, and b) the authorization to pay the specified amount of funds $X on the selected complete bill; both of which are digitally signed by the customer computer 30-m. This is indicated in Fig. 5 by reference numeral 53d.

Thereafter, the computer Y sends a message to the computer X(i) and X(j) which indicates whether or not settlement was successful. This occurs at time t10 in Fig. 5. If settlement occurred, program 52a in computer X(j) increases the biller's account by the amount of the payment which was authorized, and program 51a in computer X(i) decreases the customer's account by the amount of the payment which was authorized.

Thereafter, computer X(i) sends a message to the bill presentment computer 20 which indicates whether or not the payment as authorized in the payment request message was settled. In response, program 24 in the bill presentment computer 20 changes the status code for the bill on which payment was requested to a code of " 4" or " 5" . A code of " 4" indicates that settlement occurred; and a code of " 5" indicates that settlement was rejected.

One primary feature of the above described electronic bill processing system is that item 53d in the payment closing records 53c of the clearing and settlement computer Y provides a means for resolving disputes which can arise between a customer and a biller. In Fig. 6, a process is shown which illustrates how such disputes are resolved. All of the steps of Fig. 6 are performed by a computer Z, which is a computer that has authorization to access item 53d for the disputed bill from the payment closing records 53c of the clearing and settlement computer Y, and has authorization to access the disputed bill from the biller computer 10-n.

Initially, in step S31 of Fig. 6, computer Z sends a message to the clearing and settlement computer Y which requests item 53d from the payment closing records 53c. In response, in step S32, computer Z receives item 53d which in Fig. 6 is indicated as $S_c(\$X, S_b(H(CBILL)))$. As was previously explained, $S_b(H(CBILL))$ is a hash of a complete bill which is digitally signed by the biller computer 10-n, and $X is the amount of funds which was authorized to be paid on that complete bill. S_c indicates that both of the above items are digitally signed by the customer computer 30-m.

Next, in step S33, computer Z uses a public key for the customer computer 30-m to decrypt $S_c(\$X, S_b(HCBILL)))$. By this step, the quantities $X and $S_b(H(CBILL))$ are obtained in an unsigned form. Then in step S34, computer Z compares the quantity $X to an amount which the customer alleges that he paid. If those two quantities are not equal, then step S35a is performed wherein computer Z generates a message for a dispute resolution statement (DRS) which indicates that the customer did not pay the amount which he says he paid.

Otherwise in step S35b, computer Z generates a message for the DRS which indicates that the customer did pay the amount which he says he paid.

Next, computer Z proceeds with step S36 in which a public key for the biller computer 10-n is obtained. Then, that public key is used by computer Z to decrypt $S_b(H(CBILL))$ and thereby obtain H(CBILL) in an unsigned form. Next, in step S37, computer Z sends a message to the biller computer 10-n which requests the current complete bill, which should correspond to the complete bill that was used to generate the above decrypted hash. This current complete bill is received by computer Z in step S38; and using that current complete bill, computer Z in step S39 recomputes a new hash.

Then, in step S40, computer Z compares the hash H(CBILL) as obtained in step S36 to the new recomputed hash as obtained in step S39. If those two hashes are not equal, then computer Z performs S41a in which a message is generated for the DRS which indicates that the disputed bill was changed after the amount $X was paid on the bill. Otherwise, step S41b is performed where computer Z generates a message for the DRS which indicates that the bill has not changed since the payment of $X was made.

Finally, in step S42, computer Z generates the DRS such that it includes the messages that were generated in steps S35a, S35b, S41a, and S41b. This DRS is sent to the customer and the biller to help them resolve their differences on their disputed bill.

Also, another primary feature of the above described electronic bill processing system is that it enables any change in any particular complete bill to be

detected, even though each complete bill is only stored in a single computer, which is the biller computer 10-n. This feature is achieved by storing in the bill presentment computer 20 and the settlement computer Y, a hash of each complete bill, which is digitally signed by the biller computer. Each such digitally signed hash preferably consists of sixteen to thirty-two bytes; whereas each complete bill typically consists of thousands of bytes, as is seen from Figs. 2A & 2B. Consequently, the total amount of storage is greatly reduced in the data base 22 of the bill presentment computer 20 and in the payment closing records 53c of the clearing and settlement computer Y.

An electronic bill processing system, which constitutes one preferred embodiment of the present invention, has now been described in detail in conjunction with Figs. 1-6. In addition however, certain changes and modifications can be made to this preferred embodiment without departing from the nature and spirit of the invention.

For example, in Fig. 5, the customer computer 30-m sends the payment request message PRM to the bill presentment computer 20; and thereafter, computer 20 sends the payment request message to the electronic payment subsystem 50. This occurs at times t1 and t3 in Fig. 5. However, as a modification, the payment request message can be sent from the customer computer 30 directly to the electronic payment system 50; and this modification is shown in Fig. 7.

All of the components within the electronic payment subsystem 50 of Fig. 7 are the same as those which are shown in Fig. 5, and also their operation is the same as was previously described in conjunction with

Fig. 5. Thus, all of the reference numerals within the electronic payment subsystem 50 of Fig. 7 are the same as those shown in Fig. 5.

At time t1* in Fig. 7, the customer computer 30-m sends the payment request message directly to the electronic payment subsystem 50. No payment request message is sent to the bill presentment computer 20. Later, at time t11* in Fig. 7, the customer computer 30 receives a confirmation, or a rejection, for the payment request message from the electronic payment subsystem 50.

As another modification, the payment request message can be digitally signed by the customer computer 30-m in a different manner from that which is shown in Fig. 5; and this modification is also illustrated in Fig. 7. With the modification of Fig. 7, the hash of the selected complete bill which is signed by the biller computer, and the authorization to pay a specified amount of funds on that selected complete bill, are each signed separately by the customer computer 30-m. These two separately signed items are shown in Fig. 7 as $S_c(\$X)$ and $S_c(S_b(H(CBILL)))$. By comparison, in Fig. 5, the items $X and $S_b(H(CBILL))$ are signed as one concatenated entity by the customer computer.

As another modification to the electronic bill processing system of Figs. 1-6, the bill presentment computer 20 can be completely eliminated; and this modification is shown in Fig. 8. With the Fig. 8 modification, program 31 in the customer computer 30-m sends a request to the biller computer 10-n for a particular complete bill, which in Fig. 8 is indicated as request CBILL. In response, program 17 in the biller computer 10-n calculates the hash of the complete bill and digitally signs that hash with the biller computer's

private key " b" . This digitally signed hash $S_b(H(CBILL))$ and the requested complete bill CBILL are then sent to the customer computer 30-m.

Thereafter, program 31 in the customer computer 30-m performs the previously described steps S20-S24 of Fig. 4, whereby the complete bill is visually displayed, and a payment on the displayed bill can be authorized. If such a payment is authorized, then program 31 sends a payment request message PRM at time t1* to the electronic payment subsystem 50; and a response from the payment subsystem 50 is received at time t11*. To generate this response, all of the components within the electronic payment subsystem 50 of Fig. 8 operate the same as was previously described in conjunction with Fig. 7.

As another modification, each biller computer 10-n can periodically interact with the electronic payment subsystem 50 to automatically identify all of the bills which have not been fully paid. This modification is shown in Fig. 8, wherein a program 18 is provided in the biller computer 10-n which performs the above task.

In operation, program 18 in the biller computer 10-n sends a message to computer X(j) in the biller's bank for a list of all payments which have been received on the biller's account. Then, in response, program 52a in computer X(j) generates the requested list from data base 52b, and sends the list to the biller computer 10-n.

Thereafter, program 18 in the biller computer 10-n compares the list of payments that have been made (as indicated on the received list) with the list of payments that are due (as generated from the biller's CBILL data base 13). For each bill which is not fully paid, program 18 sends a request, to computer Z of

Fig. 6, for a corresponding dispute resolution statement DRS. These statements are then used to help determine if the unpaid bill is the fault of the customer, or the biller, or both; as indicated by steps S35a, S35b, S41a, and S41b of Fig. 6.

When a dispute resolution statement indicates that a customer did not pay the amount which he says he paid on a particular bill, then program 18 in the biller computer 10-n can electronically send a notice to the customer computer 30-m; and this notice can explain that the dispute resolution statement shows that the customer is at fault. Conversely, when a particular dispute resolution statement indicates that a bill which was originally sent to a customer somehow got changed, then the biller computer 10-n can electronically send a message to the customer acknowledging that the biller error has been caught. Such a message can be sent directly to the customer computer 30-m, or can be sent to the bill presentment computer 20 for presentment to the customer computer.

As another modification, all of the messages that are sent between the various computers 10-n, 20, 30-m, X(i), X(j), Y, and Z, can include additional information, as desired, over that which has been described in conjunction with Figs. 1-8. For example, those messages can include a payment due date, a billing period, a bill reference number, an account number, etc. An example of such additional information is illustrated at the top of the bill summary which is shown in Fig. 3.

Similarly, all of the messages which are sent between the computers 10-n, 20, 30-m, X(i), X(j), Y, and Z, can be sent on communication channels of any type. For example, the messages can be sent on communication

channels which reside in physical cables or which reside in wireless networks. Also, each message between the computers can use any form of encryption to ensure that the message is received only by the one computer to which the message was sent. Similarly, any one way hash functions (message digest, cryptographic text sum, message integrity check, etc.) can be used to generate the hashes of Figs. 1-8, and any processes can be used to generate the digital signatures of Figs. 1-8.

As another modification, the customer computer 30-m can be selected from a wide variety of electronic input/output devices. One such device is a standard personal computer; but as an alternative, the customer computer 30-m can also be a public kiosk or a laptop computer or any other hand-held communications device which is able to send and receive the messages which have been described in conjunction with Figs. 1-8.

Accordingly, it is to be understood that the present invention is not limited to the details of any one particular illustrated embodiment or modification, but is defined by the appended claims.

WHAT IS CLAIMED IS:

1. An electronic bill processing system which is comprised of:

a biller computer having a data base which stores a plurality of complete bills for a plurality of customers;

a bill presentment computer, coupled to said biller computer, having a data base which stores a summary of each complete bill and a respective hash of each complete bill which is digitally signed by said biller computer; and,

multiple customer computers, coupled to said biller computer and said bill presentment computer, wherein each particular customer computer – a) requests and receives from said bill presentment computer, a summary of a selected complete bill plus its respective digitally signed hash, and b) requests and receives from said biller computer, said selected complete bill.

2. A system according to claim 1 wherein said particular customer computer responds to the receipt of said selected complete bill by – a) generating a new hash of said selected complete bill, b) decrypting said digitally signed hash of said selected complete bill, and c) indicating that a discrepancy exists, if the decrypted digitally signed hash does not equal said new generated hash.

3. A system according to claim 1 wherein said particular customer computer also sends a payment message, to said bill presentment computer, which contains – a) said digitally signed hash of said selected complete bill, and b) an authorization to pay a specified amount of funds on said selected complete bill, both of which are digitally signed by said particular customer computer.

4. A system according to claim 3 where within said payment message, said digitally signed hash of said selected complete bill and said authorization to pay said specified amount of funds are signed as one combined entity by said particular customer computer.

5. A system according to claim 3 where within said payment message, said digitally signed hash of said selected complete bill and said authorization to pay said specified amount of funds are each signed separately by said particular customer computer.

6. A system according to claim 3 wherein said bill presentment computer responds to said payment message by storing, in its data base, said digitally signed hash of said selected complete bill and said authorization to pay a specified amount of funds on said selected complete bill, both of which are digitally signed by said

particular customer computer, as obtained from said payment message.

7. A system according to claim 3 which further includes an electronic payment subsystem that holds respective accounts that are correlated with said biller and customer computers and wherein said bill presentment computer responds to said payment message by sending a request to said payment subsystem to transfer said specified amount of funds from the account for said particular customer computer to the account for said biller account.

8. A system according to claim 7 wherein said payment subsystem stores a closing record which contains said digitally signed hash of said selected complete bill and said authorization to pay a specified amount of funds on said selected complete bill, both of which are digitally signed by said particular customer computer, as obtained from said payment message.

9. A system according to claim 7 wherein said bill presentment computer also – a) receives a response from said payment subsystem which indicates that the requested transfer has occurred or was rejected, and b) updates its data base to reflect said response.

10. A system according to claim 9 wherein said bill presentment computer also generates and sends messages to

said biller computer which indicate whether or not payment of a bill has been authorized, and whether the specified amount of funds have been transferred or were rejected in said payment subsystem.

11. A system according to claim 9 wherein said bill presentment computer also generates and sends messages to each customer computer which indicate whether or not an authorized transfer of funds has occurred or has been rejected in said payment subsystem.

12. A system according to claim 1 which further includes an electronic payment subsystem that holds respective accounts that are correlated with said biller and customer computers, and wherein said particular customer computer also sends a payment message, to said payment subsystem, which contains – a) said digitally signed hash of said selected complete bill, and b) an authorization to pay a specified amount of funds on said selected complete bill, both of which are digitally signed by said particular customer computer.

13. A system according to claim 12 where within said payment message, said digitally signed hash of said selected complete bill and said authorization to pay said specified amount of funds are signed as one combined entity by said particular customer computer.

14. A system according to claim 12 where within said payment message, said digitally signed hash of said selected complete bill and said authorization to pay said specified amount of funds are each signed separately by said particular customer computer.

15. A system according to claim 12 wherein said payment subsystem stores a closing record which contains said digitally signed hash of said selected complete bill and said authorization to pay a specified amount of funds on said selected complete bill, both of which are digitally signed by said particular customer computer, as obtained in said payment message.

16. An electronic bill processing system which is comprised of:

a biller computer which generates complete bills for a plurality of customers, and generates a respective hash of each complete bill which is digitally signed by said biller computer;

multiple customer computers, coupled to said biller computer, where each particular customer computer generates a payment message which contains – a) the hash of a selected complete bill which is digitally signed by said biller computer, and b) an authorization to pay a specified amount of funds on said selected complete bill, and where items a) and b) are both digitally signed in said payment message by said particular customer computer; and,

a payment subsystem, coupled to said customer computers, which stores a closing record that contains items a) and b) digitally signed by said particular customer computer from said payment message.

17. A system according to claim 16 and further including a dispute resolving means which: reads from said closing record, said hash of said selected complete bill which is digitally signed by said biller computer and said particular customer computer; decrypts said digitally signed hash to thereby obtain the said hash in an unsigned form; generates a new hash of an alleged complete bill; and, compares said new hash to the decrypted hash in unsigned form.

18. A system according to claim 16 and further including a dispute resolving means which: reads from said closing record, said authorization to pay a specified amount of funds which is digitally signed by said particular customer computer; decrypts said digitally signed authorization to thereby obtain said specified amount of funds in an unsigned form; and, compares said unsigned specified amount of funds to an alleged payment.

19. A system according to claim 16 where within said payment message, said hash of said selected complete bill digitally signed by said biller computer and said authorization to pay said specified amount of funds, are

signed as one combined entity by said particular customer computer.

20. A system according to claim 16 where within said payment message, said hash of said selected complete bill digitally signed by said biller computer and said authorization to pay said specified amount of funds, are each signed separately by said particular customer computer.

21. A system according to claim 16 which further includes a bill presentment computer, coupled to said biller computer and to said multiple customer computers, which stores a summary of each complete bill and stores said respective hash of each complete bill which is digitally signed by said biller computer; and, wherein each customer computer – a) requests and receives from said bill presentment computer, the summary of a selected complete bill plus its respective digitally signed hash, and b) requests and receives from said biller computer, said selected complete bill.

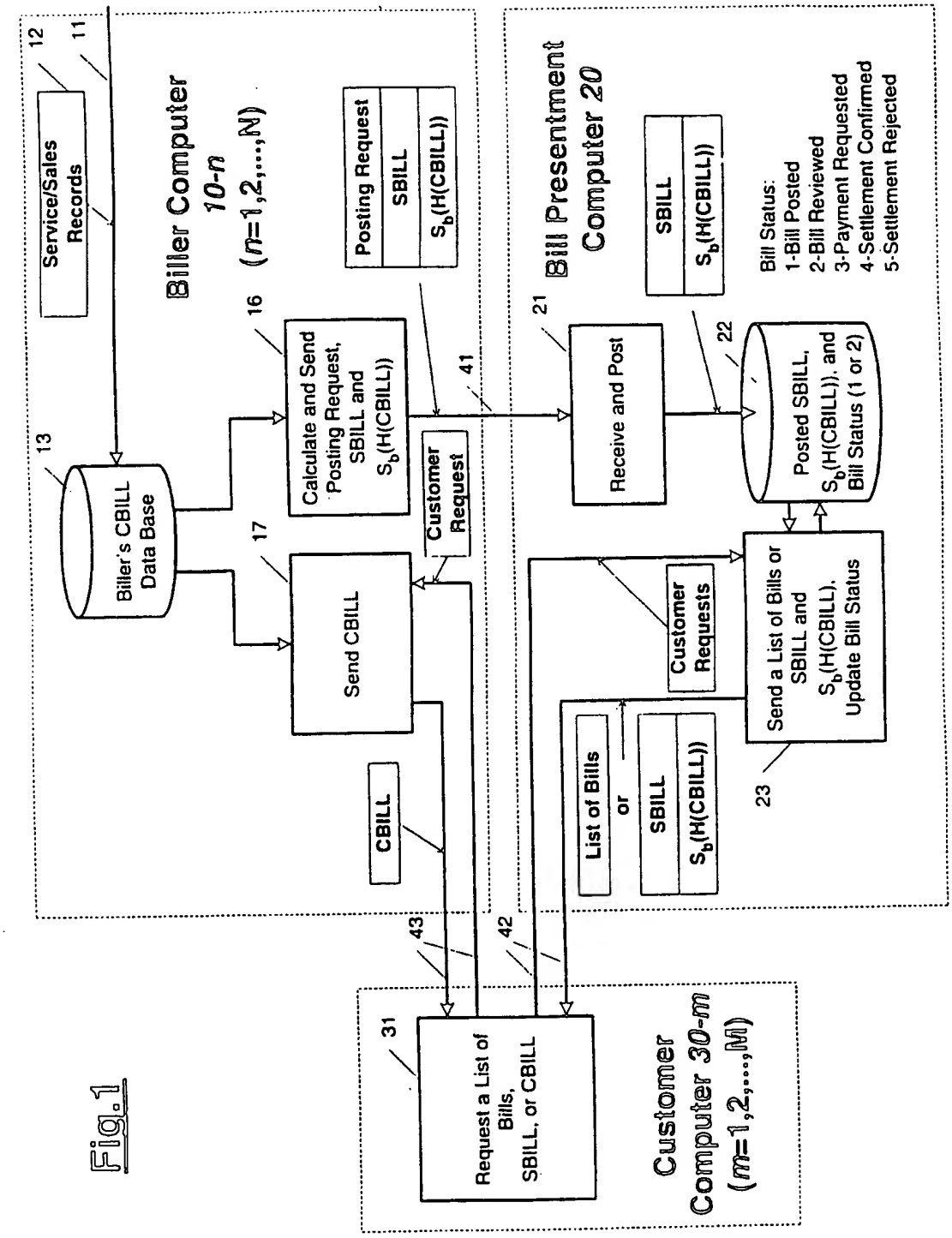

Biller Computer
10-n
(n=1,2,...,N)
Bill Presentment
Computer 20
Customer
Computer 30-m
(m=1,2,...,M)
Service/Sales
Records
12
11
13
Biller's CBILL
Data Base
16
Calculate and Send
Posting Request,
SBILL and
$S_b(H(CBILL))$
Posting Request
SBILL
$S_b(H(CBILL))$
41
21
Receive and Post
22
Posted SBILL,
$S_b(H(CBILL))$, and
Bill Status (1 or 2)
SBILL
$S_b(H(CBILL))$
Bill Status:
1-Bill Posted
2-Bill Reviewed
3-Payment Requested
4-Settlement Confirmed
5-Settlement Rejected
17
Send CBILL
Customer
Request
CBILL
Customer
Requests
Send a List of Bills or
SBILL and
$S_b(H(CBILL))$,
Update Bill Status
23
List of Bills
or
SBILL
$S_b(H(CBILL))$
43
42
31
Request a List of
Bills,
SBILL, or CBILL

Fig.1

Fig. 2A

15b

* *California Bell* *

Residence Flat Rate Serv		Statement Date	JOHN DOE	Page 1
Account Number		May 21, 1997	1234 MAIN ST	
808 677-1234	227 K 0193		IRVINE, CA 92356	
Current	California Bell		Page 1-7	545.21
Charges	NCI		Page 8-10	516.68
Total Due	Due by Jun 11, 1997			$1061.89

15c

LATE CHARGE REMINDER. A late charge may apply on June 13 if your payment has not been received. (See Reverse)

15a

Work At Home?	Do you need help setting up your home office? Do you telecommute and want to make better use of your phone service? Call Work at Home Resources at 1-800-700-1100 for a free consultation.

California Bell Calls From 808 677-1234

14a

	Date	Time	Place and Number	Called	Type	Rate	Minutes	Amount Before Discount
1.	Apr21	3:04pm	LOSANGELESCA	213 874-6611	Direct	Day	1	.15
2.	Apr21	10:47pm	BEVERLYHLS CA	310 648-9843	Direct	Eve	2	.22
3.	Apr22	11:22am	AGOURA___ CA	818 573-9984	Direct	Day	9	2.06
4.	Apr22	3:13pm	LOSANGELESCA	213 874-6611	Direct	Day	7	.29
5.	Apr23	10:31pm	BEVERLYHLS CA	310 648-9843	Direct	Eve	2	.22
6.	Apr23	11:49am	AGOURA___ CA	818 573-9984	Direct	Day	8	1.89
7.	Apr24	12:49am	AGOURA___ CA	818 573-9984	Direct	Day	9	2.06
				• • •				
255.	May 20	9:20pm	LOSANGELESCA	213 778-2249	Direct	Eve	7	.72
256.	May 20	9:30pm	LOSANGELESCA	213 426-1737	Direct	Eve	17	1.76
257.	May 20	9:55pm	RESEDA CA	818 07-5040	Direct	Eve	21	2.65
Total California Bell Calls from 808 677-1234								$531.97

Taxes & Surcharges

14b

	Description	Amount
1.	Charges for Network Access for Interstate Calling, Imposed by Federal Communications Commission	7.00
2.	CA High Cost Fund Surcharge - A:	2.21
3.	California Teleconnect Fund Surcharge	.31
4.	Universal Lifeline Telephone Service Surcharge	2.47
5.	Rate Surcharge	2.37CR
6.	State Regulatory Fee	.08
7.	CA Relay Service and Communications Devices Fund	.28
8.	Tax: Fed: 2.65 911: .59 Local:	3.24
Total Taxes and Surcharges		$13.24

Fig. 2B

Account Number
808 677-1234 235 S 0182
NCI Account Number
7Q633529

Statement Date
May 21, 1997
Questions about your NCI bill?
800-266-9963

Page 8

✳NCI✳✳ ☎

15c

Long Distance

Calls from 808 677-1234:

	Date	Time	Place and Number Called		Type	Rate+	Minutes	Amount
1.	Apr 21	7:25pm	SAN JOSE CA	408 244-1977	Direct	Eve	1	.09
14c 2.	Apr 21	7:38pm	FAIR LAWN NJ	201 705-3304	Direct	Eve	1	.14
			•					
			•					
			•					
83.	May 20	4:30pm	RIDLEYPARKPA	610 592-1293	Direct	Day	8	1.97
Total Calls from 808 677-1234								202.20
Total Long Distance								202.20

International Long Distance

NCI Savings™ plan from 808 677-1234:

	Date	Time	Place and Number Called		Type	Rate+	Minutes	Amount
1.	Apr 21	9:34am	RUSSIA	70957832217	Direct	Std	4	4.77
14d 2.	Apr 21	9:40pm	Ukraine	70957832217	Direct	Eve	2	2.38
			•					
			•					
			•					
55.	May 21	9:44pm	RUSSIA	70956166486	Direct	Eve	3	3.57
Total NCI Savings™ plan from 808 677-1234								310.72
Total International Long Distance.								310.72

Taxes and Surcharges

Federal Excise Tax	.49
State and Local Taxes	.02
14e State & Local Surcharges	.04
Universal Lifeline Telephone Services	.10
California Relay Service and Communications Devices Fund	.01
California High Cost Fund-B Surcharge	.09
California Teleconnect Fund	.01
Total Current Taxes and Surcharges	.76

Service Summary

NCI Savings™ plan (03/28/97 to 10/27/97)	3.00
Long Distance	202.20
Inernational Long Distance.	310.72
Total Current Charges	515.92

Fig. 3

Service/ Biller	Account Number	Bill Reference Number (ID)	Current Charges, $	Payment Due By, mm/dd/ yyyy	Billing Period From, mm/dd/ yyyy	Billing Period To, mm/dd/ yyyy	Past Due Amount, $	Comments
California Bell	808 677-1234 227 K 0193	may211997	1061.89	06/11/ 1997	04/21/ 1997	05/20/ 1997	0	

Display Complete Bill	*Display Payment Screen*	*Return to LCUB*	*End*

Fig. 4

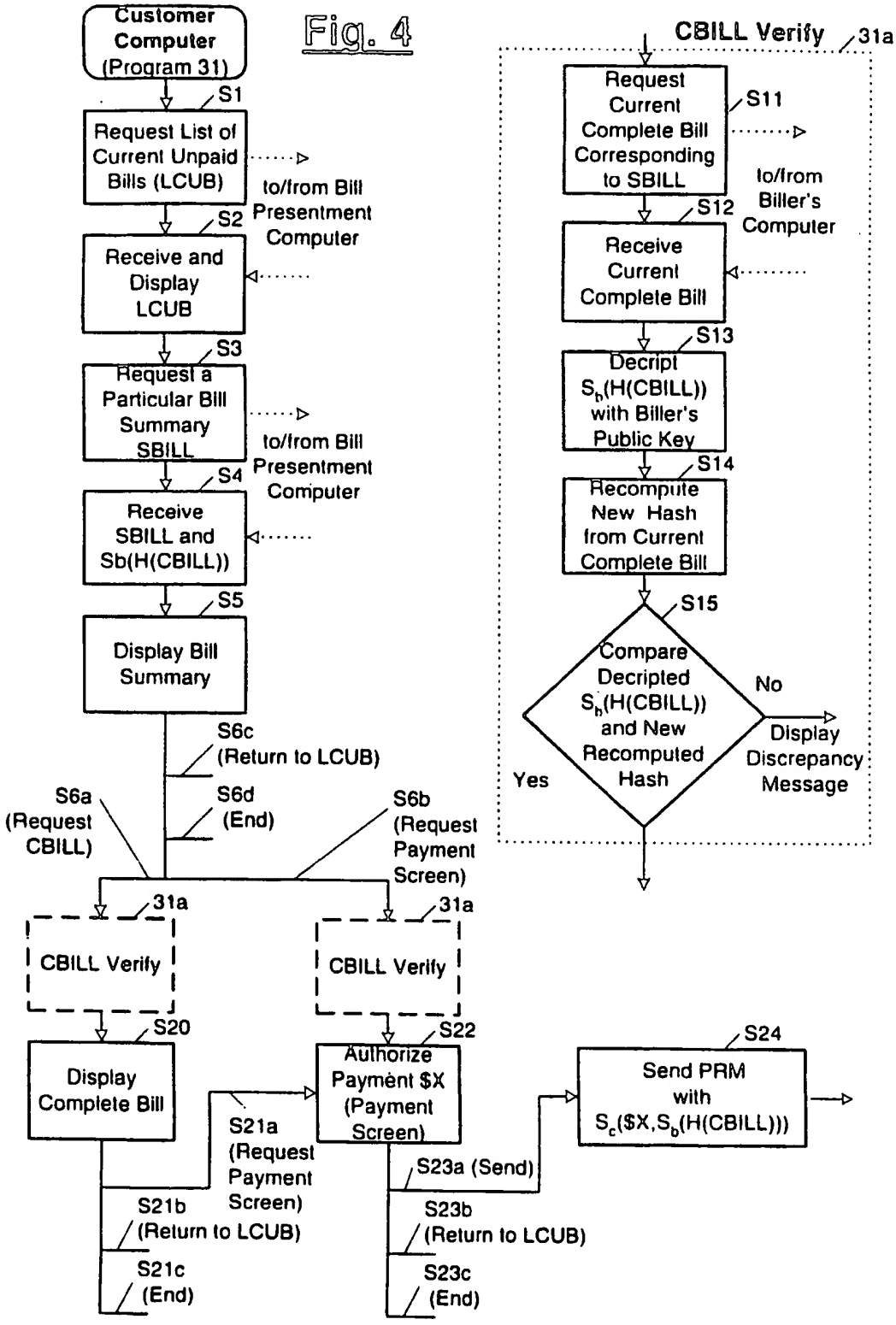

Customer Computer (Program 31)
S1
Request List of Current Unpaid Bills (LCUB)
to/from Bill Presentment Computer
S2
Receive and Display LCUB
S3
Request a Particular Bill Summary SBILL
to/from Bill Presentment Computer
S4
Receive SBILL and Sb(H(CBILL))
S5
Display Bill Summary
S6c (Return to LCUB)
S6a (Request CBILL)
S6d (End)
S6b (Request Payment Screen)
31a
CBILL Verify
31a
CBILL Verify
S20
Display Complete Bill
S22
Authorize Payment $X (Payment Screen)
S24
Send PRM with Sc($X,Sb(H(CBILL)))
S21a (Request Payment Screen)
S21b (Return to LCUB)
S21c (End)
S23a (Send)
S23b (Return to LCUB)
S23c (End)
CBILL Verify
31a
Request Current Complete Bill Corresponding to SBILL
S11
to/from Biller's Computer
S12
Receive Current Complete Bill
S13
Decript Sb(H(CBILL)) with Biller's Public Key
S14
Recompute New Hash from Current Complete Bill
S15
Compare Decripted Sb(H(CBILL)) and New Recomputed Hash
No
Display Discrepancy Message
Yes

Fig. 5

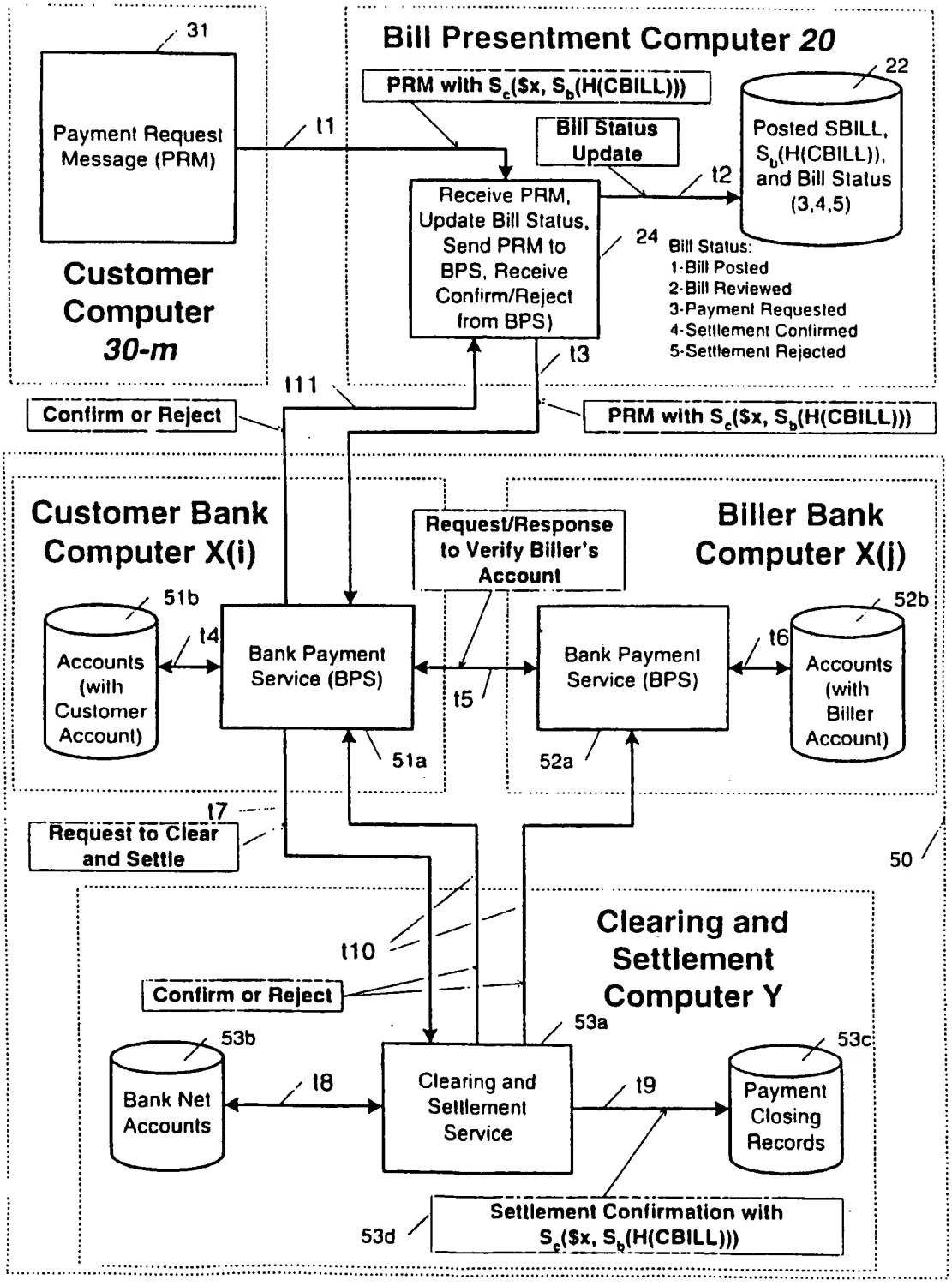

31
Payment Request Message (PRM)
Customer Computer 30-m
t1
Bill Presentment Computer 20
PRM with $S_c($x, $S_b(H(CBILL)))$
Bill Status Update
22
Posted SBILL, $S_b(H(CBILL))$, and Bill Status (3,4,5)
t2
Receive PRM, Update Bill Status, Send PRM to BPS, Receive Confirm/Reject from BPS)
24
Bill Status:
1-Bill Posted
2-Bill Reviewed
3-Payment Requested
4-Settlement Confirmed
5-Settlement Rejected
t3
t11
Confirm or Reject
PRM with $S_c($x, $S_b(H(CBILL)))$
Customer Bank Computer X(i)
Request/Response to Verify Biller's Account
Biller Bank Computer X(j)
51b
Accounts (with Customer Account)
t4
Bank Payment Service (BPS)
t5
Bank Payment Service (BPS)
t6
52b
Accounts (with Biller Account)
51a
52a
t7
Request to Clear and Settle
50
Clearing and Settlement Computer Y
t10
Confirm or Reject
53a
53b
Bank Net Accounts
t8
Clearing and Settlement Service
t9
53c
Payment Closing Records
53d
Settlement Confirmation with $S_c($x, $S_b(H(CBILL)))$

Fig. 6

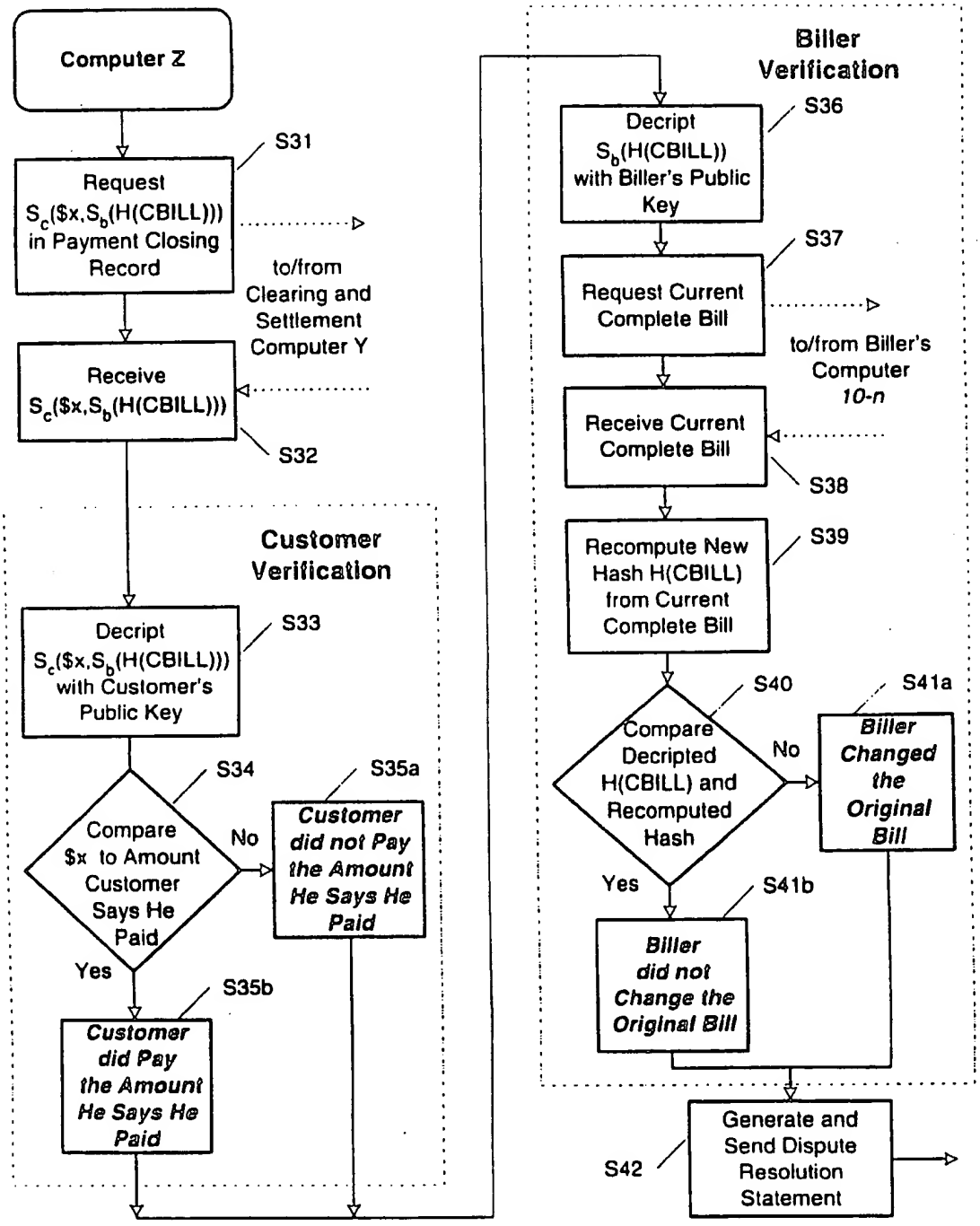

Computer Z
S31
Request $S_c($x,$S_b(H(CBILL)))$ in Payment Closing Record
to/from Clearing and Settlement Computer Y
Receive $S_c($x,$S_b(H(CBILL)))$
S32
Customer Verification
Decript $S_c($x,$S_b(H(CBILL)))$ with Customer's Public Key
S33
S34
Compare $x to Amount Customer Says He Paid
No
S35a
Customer did not Pay the Amount He Says He Paid
Yes
S35b
Customer did Pay the Amount He Says He Paid
Biller Verification
S36
Decript $S_b(H(CBILL))$ with Biller's Public Key
S37
Request Current Complete Bill
to/from Biller's Computer 10-n
Receive Current Complete Bill
S38
Recompute New Hash H(CBILL) from Current Complete Bill
S39
S40
Compare Decripted H(CBILL) and Recomputed Hash
No
S41a
Biller Changed the Original Bill
Yes
S41b
Biller did not Change the Original Bill
S42
Generate and Send Dispute Resolution Statement

Fig. 7

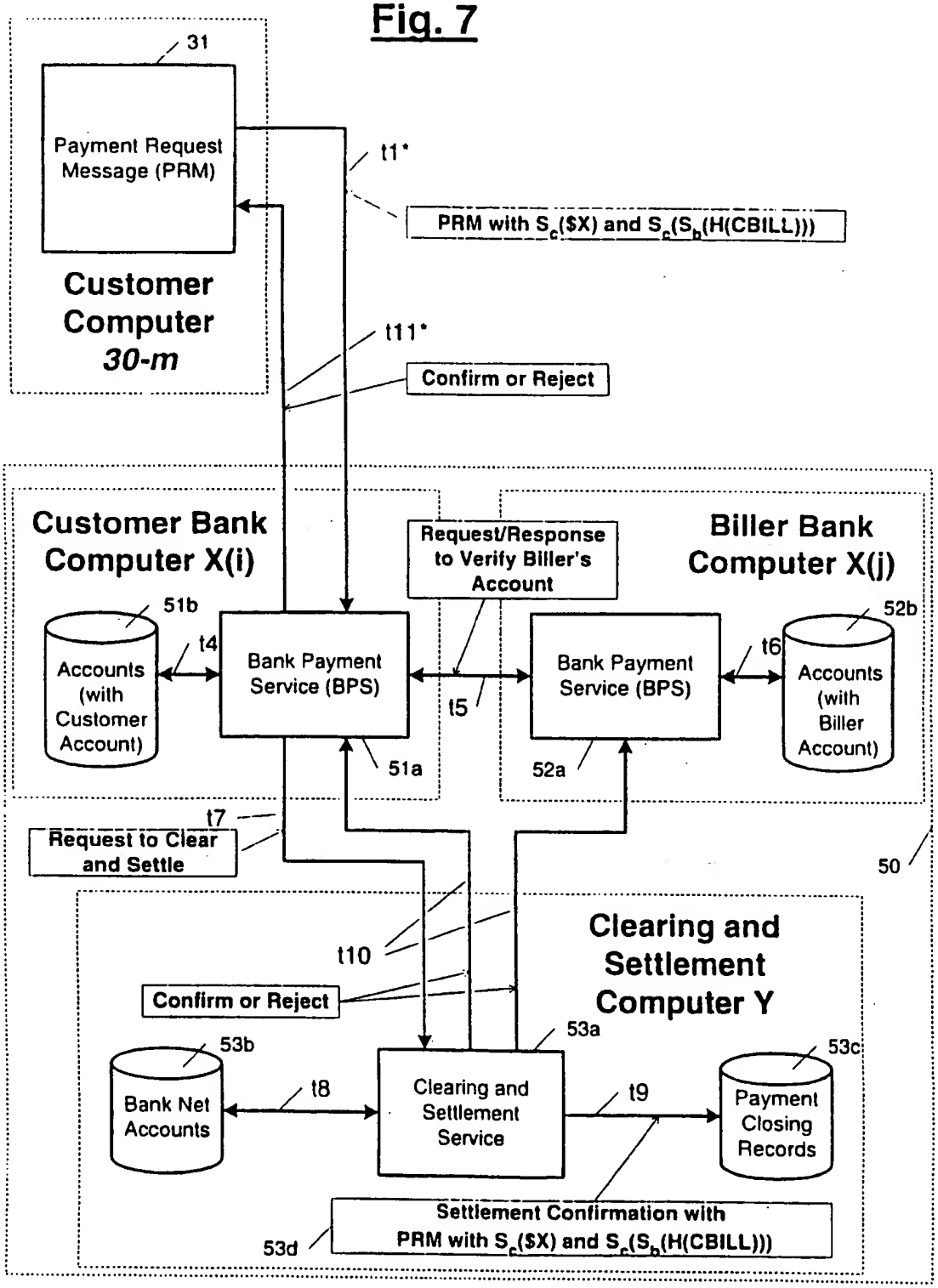
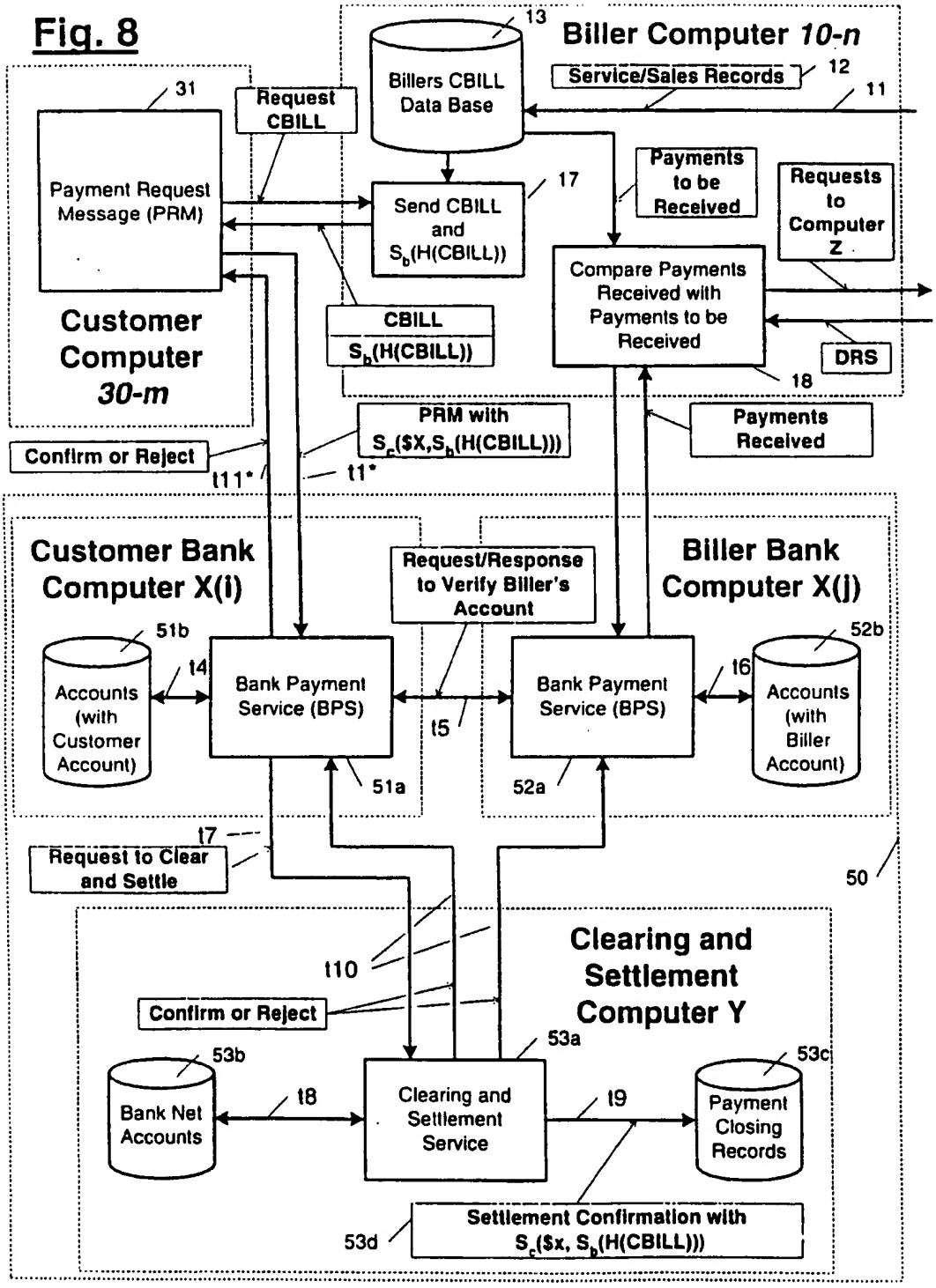

31
Payment Request Message (PRM)
Customer Computer 30-m
t1*
PRM with $S_c($X) and $S_c(S_b(H(CBILL)))
t11*
Confirm or Reject
Customer Bank Computer X(i)
Request/Response to Verify Biller's Account
Biller Bank Computer X(j)
51b
Accounts (with Customer Account)
t4
Bank Payment Service (BPS)
t5
Bank Payment Service (BPS)
t6
52b
Accounts (with Biller Account)
51a
52a
t7
Request to Clear and Settle
50
Clearing and Settlement Computer Y
t10
Confirm or Reject
53a
53b
Bank Net Accounts
t8
Clearing and Settlement Service
t9
53c
Payment Closing Records
Settlement Confirmation with PRM with $S_c($X) and $S_c(S_b(H(CBILL)))
53d

Fig. 8


Biller Computer 10-n
13
Billers CBILL Data Base
Service/Sales Records
12
11
31
Request CBILL
Payment Request Message (PRM)
Send CBILL and $S_b(H(CBILL))$
17
Payments to be Received
Requests to Computer Z
Compare Payments Received with Payments to be Received
DRS
18
Customer Computer 30-m
CBILL
$S_b(H(CBILL))$
PRM with $S_c(\$X, S_b(H(CBILL)))$
Payments Received
Confirm or Reject
t11*
t1*
Customer Bank Computer X(i)
Request/Response to Verify Biller's Account
Biller Bank Computer X(j)
51b
52b
Accounts (with Customer Account)
t4
Bank Payment Service (BPS)
t5
Bank Payment Service (BPS)
t6
Accounts (with Biller Account)
51a
52a
t7
Request to Clear and Settle
50
Clearing and Settlement Computer Y
t10
Confirm or Reject
53a
53b
53c
Bank Net Accounts
t8
Clearing and Settlement Service
t9
Payment Closing Records
53d
Settlement Confirmation with $S_c(\$x, S_b(H(CBILL)))$

INTERNATIONAL SEARCH REPORT

Int ational Application No
PCT/US 98/15190

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F17/60

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	WO 98 26364 A (SUN MICROSYSTEMS, INC) 18 June 1998 see abstract see page 3, last paragraph - page 5, paragraph 1 see page 6, paragraph 2 - page 8, paragraph 3 ---	16
Y	EP 0 745 947 A (IBM CORPORATION) 4 December 1996	16
A	see abstract see column 3, paragraph 2 - column 4, paragraph 1 --- -/--	1-15, 17-21

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publicationdate of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of theinternational search	Date of mailing of the international search report
20 November 1998	27/11/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Skulikaris, I

3

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int ational Application No
PCT/US 98/15190

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication,where appropnate, of the relevant passages	Relevant to claim No.
Y	SIRBU ET AL: "NetBill: An Internet Commerce System Optimized for Network-Delivered Services" IEEE PERSONAL COMMUNICATIONS, vol. 2, no. 4, August 1995, pages 34-39, XP000517588	16
A	see page 35, left-hand column, last paragraph - page 36, right-hand column, paragraph 1 see page 37, left-hand column, paragraph 6 - page 38, left-hand column, paragraph 1 ---	1-15, 17-21
A	US 5 649 117 A (MIDWEST PAYMENT SYSTEMS) 15 July 1997 see column 7, paragraph 2 see column 12, paragraph 3 see column 19, paragraph 4 see column 33, paragraph 3 -----	1-21

3

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. ional Application No
PCT/US 98/15190

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9826364 A	18-06-1998	NONE	
EP 0745947 A	04-12-1996	US 5832460 A	03-11-1998
		CA 2173713 A	03-12-1996
		CN 1141454 A	29-01-1997
US 5649117 A	15-07-1997	NONE	